BURSOR & FISHER, P.A.
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: jsmith@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KATRINA CALDERON and DANIELLE CALDERON, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

NATURE OF THE ACTION

1. This is a putative class action against Defendant Meta Platforms, Inc., fka Facebook, Inc. ("Meta" or "Facebook") for wiretapping electronic communications on major on-line tax filing websites offered by H&R Block, TaxAct, and TaxSlayer. As a result of this wiretapping, U.S consumers have been transmitting their sensitive financial information to Meta when they file their taxes online. This information has included things like income, refund amounts, filing status, the names of dependents, and scholarship information.

2. The device that made this wiretapping possible is Meta's ubiquitous tracking pixel, which is embedded in the JavaScript of online tax preparation websites, and which is part of a larger set of free "business tools" that Meta offers to website owners. This pixel gathers information from website visitors even if they do not have a Meta account.

3. Disclosing tax-return information without consent is a crime. 26 U.S. § 7216. Aiding and abetting the unlawful disclosure of tax-return information is a crime. Inspecting unlawfully obtained tax-return information is a crime. 26 U.S. § 7213A(a)(2).

4. This action is brought on behalf of Plaintiffs and a putative class of all people in the United States who used the online tax preparation providers H&R Block, TaxAct, or TaxSlayer while those websites had the Meta pixel installed on them. This action also seeks to certify a putative subclass of Californians who used the same websites. The complaint alleges violations of state and federal wiretapping laws.

THE PARTIES

5. Plaintiff Katrina Calderon is domiciled in California and lives in Salinas. For the year 2021, Ms. Calderon used TaxAct's website to file her taxes online. At that time, the website utilized Facebook's tracking pixel. Ms. Calderon also has a Facebook account.

6. Plaintiff Danielle Calderon is domiciled in California and lives in Castro Valley. For the year 2021, Ms. Calderon used Tax Slayer's website to file her taxes online. At that time, the website utilized Facebook's tracking pixel. Ms. Calderon also has a Facebook account.

7. Meta is a California corporation with its headquarters in Menlo Park, California. Facebook does business throughout California.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this class action. This Court has personal jurisdiction over Meta because it is headquartered in this State.

9. Venue is proper in this Court because Meta conducts business in this County and throughout the State of California and its principal place of business is in this County.

STATEMENT OF FACTS

The Evolution Of Meta's Business Model: From Social Media to Surveillance

10. Meta operates Facebook.com, and is the world's largest social media company.

11. Within 10 months of Facebook.com's initial launch, the site reached 1 million active users, quickly swelling to 30 million less than three years later. As its user base grew, so too did interest from investors. By late 2007, interest turned to clamor, and after rejecting a steady flow of proposed investments and buyouts, Meta (then called "Facebook") settled on an offer from Microsoft, agreeing to a $240 million investment for a 1.6 percent stake, which extrapolated to an eye-popping valuation: $15 billion.

12. Commentators scrutinized the deal, pointing to the gaping disparity between Facebook's valuation and its revenue. "When a startup shows an estimated $150 million in revenue, isn't wildly profitable, and doesn't have a clear revenue model, no company in its right mind would give it a $15 billion valuation – except, it seems, if we're talking about Facebook." In short order, Meta/Facebook set about crafting that revenue model.

13. Because Facebook offered access to its platform for free, users were exactly that—users, not customers. Rather than find a way to make them customers, Facebook made them the products. Facebook planned to mine its platform and third-party websites for insights it could use to target and customize advertisements for businesses. User activity served as the raw materials that Facebook analyzed and dissected for inferences answering its ultimate question: what advertisement, from which company, for which user, will have maximal impact. The better Facebook could answer that question, the better it could "improve the effectiveness of the ads and recruit new advertisers who want to pitch their messages to refined slices of the online audiences." Facebook announced this new business model on November 6, 2007.

14. As that date approached, details leaked about its soon-to-be launched advertising system, with one clear takeaway: "***Facebook is going to be gunning hard to get lots and lots of third-party data about its users into its database***." On November 6, 2007, Facebook unveiled its new ad system, "Facebook Ads," pitching it as a way "for businesses to connect with users and target advertising to the exact audiences they want." The new system had three component parts: Social Ads, which let businesses build Facebook pages and create advertisements featuring a user's interaction with those pages; Insights, which let businesses track how those social ads spread among users; and the Beacon program.

15. In 2021, Meta generated $117 billion in revenue. Roughly 97% of that came from selling advertising space.

16. Meta sells advertising space by highlighting its ability to target users.

17. Meta describes itself as a "real identity platform," meaning users are allowed only one account and must share "the name they go by in everyday life." To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.

18. Meta maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications that Meta associates with personal identifiers including IP addresses, cookies, and device identifiers.

19. Meta can target users so effectively because it surveils user activity both on and off its site. This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections." Meta compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.

The Wiretapping Device: Meta's Tracking Pixel

20. Meta offers a suite of so-called Business Tools that it claims "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."

21. One of those tools is Meta's pixel, which is an invisible 1x1 web bug that website

owners can install on their websites to measure certain actions taken by users on their own websites, such as online purchases.

22. Meta describes its pixel as follows: "The Meta Pixel is a snippet of JavaScript code ***that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a conversion)***. Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels."

23. The pixel has vast capabilities and can collect a large range of user data, including, the following, according to Meta:

- **HTTP Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.
- **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
- **Button Click Data** – Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.
- **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
- **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.

24. In May 2017, Meta added new functionality to "enhance" its tracking abilities by transmitting additional information to Facebook, including "actions on your page" and additional information about the website structure to better understand the context associated with any actions that are tracked. The new information also included button click data and page metadata from websites. The enhancements were automatically implemented to all pixels, including those that were installed on websites before the enhancements were available.

25. The website communications collected by the tracking pixel are transmitted in real time to Meta's servers, where the information is stored. The information also is transmitted to Meta while it is being sent from or received within California.

26. Meta explains "How the Facebook Pixel Works" in relevant part as follows: "When someone visits your website and takes an action (for example, buying something), ***the Facebook pixel is triggered and reports this action***. This way, you'll know when a customer took an action after seeing your Facebook ad."

27. Meta has stated that "When someone takes an action that the [website] developer has chosen to measure on its website, ***the Meta Pixel is triggered and sends Meta certain data,*** called an 'Event.' Meta attempts to match the Events it receives to Meta users. The developer can then choose to show ads to users who have taken a certain action on their own website."

28. Meta has stated that the tracking pixel "***log[s] when someone takes an action***" such as "adding an item to their shopping cart or making a purchase."

29. As soon as a website user takes any action on a webpage which includes the tracking pixel—such as clicking a button to register, login, or logout of a website, Meta's source code commands the user's device to re-direct the content of the communication to Meta while the exchange of the communication between the user and the website is still occurring.

30. By design, Meta receives the content of website communications as the website user enters the information but before the website owner receives it.

31. The Meta pixel matches website users to their corresponding Facebook.com profile.

32. The tracking pixel utilizes "Automatic Advanced Matching." Automatic Advanced Matching enables the Meta pixel to "look for recognizable form field and other sources on your website that contain information such as first name, last name and email." The tracking pixel then intercepts and transmits that information, "along with the event, or action, that took place."

33. Meta also uses various cookies to supplement the tracking pixel's tracking practices. Specifically, the pixel contains a script that causes the user's browser to transmit to Meta information from each of the Meta cookies already existing on the browser's cache.

34. Meta intercepts and collects this information so it can better match visitors to their

Facebook.com profiles, which in turn allows tax filing companies to better target their advertisements.

35. Meta intercepts and collects information from its pixel regardless of whether a user is logged into Facebook.com or has ever registered for an account.

36. Even if a user is not logged in, Meta can still associate the data with their IP address and all the websites that they have been to that contain the tracking pixel.

37. After collecting and intercepting this information, Meta processes it, analyzes it, and assimilates it into datasets like Core Audiences.

38. Meta's tracking pixel is not simply a "tool" utilized by website owners for their own purposes. Meta offers these technologies to companies for free because Facebook benefits too. Meta says it can use the data it gleans from tools like the pixel to power its algorithms, providing it insight into the habits of users across the internet. Indeed, the data obtained allows Meta to amass huge amounts of data in a detailed dossier, or digital fingerprint, that it keeps on its users and other website visitors.

39. Meta uses data obtained from the tracking pixel to target users with advertisements based on their interests. For example, Meta admitted that "[w]e use the information we have (including your activity off our Products, such as the websites you visit and the ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services."

40. In short, Meta uses the data that it collects from the pixel to increase its ad revenue.

41. The pixel is widely deployed across many industries.

42. The pixel has been available to website developers since at least October 14, 2015.

Meta Secretly Hoovers Up Vast Amounts Of Private Tax Return Information

43. Thanks to Meta's pixel and business tools, the tax filing services H&R Block, TaxAct, and TaxSlayer have been quietly transmitting sensitive financial information to Meta when Americans file their taxes online.

44. The information sent to Meta can be used by the company to power its advertising

algorithms and is gathered regardless of whether the person using the tax filing service has an account on Meta or other platforms operated by its owner, Meta.

45. H&R Block, TaxAct, and TaxSlayer are some of the most widely used e-filing services that had the tracking pixel deployed on their websites.

46. The type of data includes names and email addresses, data on users' income, filing status, refund amounts, and dependents' college scholarship amounts.

47. For example, a recently published report found that the pixel on TaxAct's website sent users' filing status, adjusted gross income, and the amount of refund to Meta. TaxAct has about three million users. Plaintiff Katrina Calderon was one of those users when she filed her taxes this year for 2021. Since the tracking pixel was on the site at that time, and it operates always and for everyone, Plaintiff Katrina Calderon's tax return data would have been sent to Meta.

48. H&R Block, which also has millions of users, reportedly transmitted information about tax filers' health savings account usage and dependents' college tuition grants and expenses.

49. TaxSlayer reportedly used the Meta tracking pixel's "advanced matching" system described above to transmit phone numbers, filer names, and the names of any dependents added to the return. TaxSlayer completed 10 million federal and state tax returns last year. Plaintiff Danielle Calderon was one of those users when she filed her taxes this year for 2021. Since the tracking pixel was on the site at that time, and it operates always and for everyone, Plaintiff Danielle Calderon's tax return data would have been sent to Meta.

50. Meta would have known, or at best recklessly turned a blind-eye, to the fact that it was collecting vast amounts of confidential tax information. Income and other related financial information is a highly valuable demographic marker for advertising purposes.

51. Meta hires account managers or representatives to help website developers and owners use the Meta Pixel and other tools. It is especially important to Meta to assist high-traffic websites that provide advertising revenue to Meta. Through its account managers and representatives, Meta would have been aware that it was receiving confidential tax and income information.

Facebook Did Not Receive Consent To Receive Confidential Tax Information

52. In litigation, Meta's position is that it has consent from Facebook.com users to obtain any information whatsoever that users disclose on third-party websites—no matter how sensitive or confidential, and even if the information is illegal to disclose.

53. In litigation, Meta's position is that consent from Facebook.com users is derived from disclosures made in its Terms of Service, Data Policy, and Cookies Policy, and regardless of whether users saw those policies.

54. Meta's Terms of Service has never specifically indicated that Meta may acquire confidential tax information obtained from Facebook users' interactions on third-party online tax preparation sites, like those offered by H&R Block, TaxAct, and TaxSlayer.

55. Meta's Data Policy has never specifically indicated that Meta may acquire confidential tax information obtained from Facebook users' interactions on third-party online tax preparation sites, like those offered by H&R Block, TaxAct, and TaxSlayer.

56. Meta's Cookies Policy has never specifically indicated that Meta may acquire confidential tax information obtained from Facebook users' interactions on third-party online tax preparation sites, like those offered by H&R Block, TaxAct, and TaxSlayer.

57. Meta also makes false representations warranties that it does not collect sensitive information like the information at issue here.

58. Meta's Business Tool Terms expressly provide that website developers will not share data that they "know ore reasonably should know … includes health, ***financial*** or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines." However, Meta does not enforce this policy.

59. In Meta's Advertising Policy, Meta states "[w]e do not use sensitive personal data for ad targeting." That statement is false.

60. In a blog post titled "About Restricted Meta Business Tools Data," Meta states, falsely, that it does not "want websites or apps sending us sensitive information about people." Sensitive information includes "any information defined as sensitive under applicable laws, regulations and applicable industry guidelines."

61. In an article titled, "How does Facebook receive information from other businesses and organizations," Meta reiterates its promise to "prohibit businesses or organizations from sharing sensitive information with us," and if Meta "determine[s] that a business or an organization is violating our terms, we'll take action against that business or organization." Those statements are false.

62. In another article, titled, "How does Meta work with data providers?" Meta states, "[b]usinesses that advertise on Facebook are required to have any necessary rights and permissions to use this information, as outlined in our Custom Audience Terms that businesses must agree to." Meta does not enforce this policy.

CLASS ACTION ALLEGATIONS

63. Plaintiffs seek to represent the following classes:

> Nationwide Class: All people in the United States who used the online tax preparation providers H&R Block, TaxAct, or TaxSlayer while those websites had the Facebook pixel installed on them.
>
> California Class: All people in California who used the online tax preparation providers H&R Block, TaxAct, or TaxSlayer while those websites had the Facebook pixel installed on them.

64. Plaintiffs reserve the right to modify the class definition, including by using subclasses, as appropriate based on further investigation and discovery obtained in the case.

65. Members of the putative class and subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the putative class and subclass number in the millions. The precise number of putative class and subclass members and their identities are unknown at this time but may be determined through discovery. Putative class and subclass members may be notified of the pendency of this action by mail and/or publication through the distribution records of Meta.

66. Common questions of law and fact exist as to all putative class and subclass members and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to, whether Defendant has violated wiretapping statutes at issue here; and whether class members are entitled to statutory damages for the

violations.

67. The claims of the named Plaintiffs are typical of the claims of the putative class and subclass because the named Plaintiffs, like all other class members, visited the websites of H&R Block, TaxAct, or TaxSlayer and had their electronic communications intercepted and disclosed to Facebook using the tracking pixel and/or other business tools.

68. Plaintiffs are adequate representatives of the putative class and subclass because her interests do not conflict with the interests of the class members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of putative class and subclass members will be fairly and adequately protected by Plaintiff and her counsel.

69. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of putative class and subclass members. Each individual putative class and subclass member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

70. Plaintiffs bring all claims in this action individually and on behalf of members of the putative class and subclass against Defendant.

COUNT I
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 631

71. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

72. Plaintiffs bring this claim individually and on behalf of the members of the putative

class and subclass against Defendant.

73. To establish liability under section 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> Or
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> Or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

74. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

75. The tracking pixel and related business tools are a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

76. At all relevant times, by using the Facebook Tracking Pixel, Defendant intentionally

tapped, electrically or otherwise, the lines of internet communication between Plaintiff and class members and the owners of the websites at issue here.

77. At all relevant times, by using the Facebook Tracking Pixel, Defendant willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff and putative class members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

78. Plaintiffs and putative class and subclass members did not consent to any of Defendant's actions in implementing the wiretaps. Plaintiffs and putative class and subclass members did not consent to Facebook's access, interception, reading, learning, recording, and collection of Plaintiffs and putative class and subclass members' electronic communications.

79. Plaintiffs and putative class and subclass members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632

80. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

81. Plaintiffs bring this Count individually and on behalf of the members of the putative class and subclass.

82. The California invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.
>
> Cal. Penal Code § 630.

83. California Penal code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop

> upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500) per violation.

84. A defendant must show it had the consent of all parties to a communication.

85. Meta's pixel and related backend and frontend code is "an electronic amplifying or recording device" under the CIPA.

86. The data collected by Meta constitutes "confidential communications," as that term is used in Section 632, because class members had objectively reasonable expectations of privacy with respect to their tax filing information.

87. Pursuant to Cal. Penal Code § 637.2, Plaintiff and class members have been injured by the violations of Cal. Penal Code § 635, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT III
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 635

88. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

89. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclass members against Defendant.

90. California Penal Code § 635 provides, in pertinent part:

> Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6 , shall be punished by a fine not exceeding two thousand five hundred dollars ….

91. At all relevant times, by implementing Meta's wiretaps, Meta intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended

for eavesdropping upon the communication of another.

92. The Facebook Tracking Pixel is a "device" that is "primarily or exclusively designed" for eavesdropping. That is, the Facebook Tracking Pixel is designed to gather information about what URLs users visit and what they search for.

93. Plaintiffs and putative class and subclass members did not consent to any of Defendant's actions in implementing Facebook's wiretaps.

94. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and putative class and subclass members have been injured by the violations of Cal. Penal Code § 635, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT IV
Violation Of The Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*

95. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

96. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclass members against Defendant.

97. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communications through the use of a device. 18 U.S.C. § 2511.

98. The Wiretap Act protects both the sending and receiving of communications.

99. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

100. Meta's actions in intercepting and tracking the information at issue here was intentional, and done for the purpose of violating laws prohibiting the unlawful disclosure and review of tax information.

101. Meta's intentional interception of internet communications that Plaintiff and Class members were sending and receiving while navigating websites that integrated Facebook's Business Tools was done contemporaneously with the Plaintiffs' and Class members' sending and receipt of those communications.

102. The communications intercepted by Meta included "contents" of electronic communications made from Plaintiffs.

103. The transmission of data between Plaintiffs and Class members were "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetics, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

104. Meta's pixel and business tools are "devices" within the meaning of 18 U.S.C. 2510(5):

105. Meta was not an authorized party to the communications because Plaintiffs and Class members were unaware of Meta's monitoring. Class members did not consent to Meta's interception or continued gathering of the user's communications.

106. The interception by Meta were unlawful and tortious, and were done in furtherance of one or more crimes baring disclosure or review of confidential tax information, and tortious invasion of privacy.

107. After intercepting the communications, Meta used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(a).

108. Plaintiffs seek all available relief for the violations asserted here.

COUNT IV
Violation Of The Federal Wiretap Act, 18 U.S.C. § 2512

109. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

110. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclass against Defendant.

111. 18 U.S.C. § 2512, in pertinent part, holds "any person" liable who manufactures, assembles, or sells "any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious

interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. 18 U.S.C. § 2512(1)(b).

112. The technology at issue here is an "electronic, mechanical, or other device" as defined by 18 U.S.C. § 2510(5), and is primarily useful for the purpose of the surreptitious interception of electronic communications.

113. Defendant manufactured, marketed, and sold its technology with knowledge that it would primarily be used to illegally intercept electronic communications.

114. Defendant conduct violated 18 U.S.C. § 2512 and therefore gives rise to a claim under 18 U.S.C. § 2520.

115. Pursuant to 18 U.S.C. § 2520, Plaintiffs and the putative class and subclass are entitled to the greater of actual damages or statutory damages or not less than $100 a day for each day of violation or $10,000, whichever is greater.

COUNT V
Invasion of Privacy (Common Law and Constitutional)

116. Plaintiffs repeat the allegations contained in the above paragraphs as if fully set forth here.

117. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclass against Defendant.

118. Article I, section I of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, and privacy."

119. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone. … It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

120. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Facebook.

121. As described herein, Meta has intruded upon the following legally protected privacy interests:

a. The Federal Wiretap Act as alleged herein;

b. The California Wiretap Act as alleged herein;

c. A Fourth Amendment right to privacy contains on personal computing devices, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California;*

d. The California Constitution, which guarantees Californians the right to privacy;

e. Facebook's Data Usage Policy, Cookie Policy, and Terms of Use, and other public promises it made not to track or intercept class members' sensitive or unlawfully-disclosed communications;

f. Federal and state statutory prohibitions on the disclosure or review of tax information

122. Class members had a reasonable expectation of privacy under the circumstances in that they could not reasonably expect Meta to commit acts in violation of federal and state civil and criminal laws; and Meta affirmatively promised users it would not track their communications or access their computer devices or web-browser when they sent or received sensitive or otherwise protected information, like their personally identifiable information.

123. Meta's actions constituted a serious invasion of privacy in that:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices;

b. Violated several federal criminal laws, including the Wiretap Act;

c. Violated state criminal laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

d. Invaded the privacy rights of tens of millions of Americans (including Plaintiff and the Class members) without their consent;

e. Constituted the taking of valuable information from tens of millions of Americans through deceit; and

f. Violated several federal criminal laws prohibiting the disclosure and review of tax information.

124. Committing criminal acts against tens of millions of Americans constitutes an egregious breach of social norms that is highly offensive.

125. Meta's intentional intrusion into class members' internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that Meta violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

126. The taking of personally identifiable information from tens of millions of Americans through deceit is highly offensive behavior.

127. Secret monitoring of a video platform is highly offensive behavior.

128. Wiretapping and surreptitiously recording of communications is highly offensive behavior.

129. Meta lacked a legitimate business interest in tracking users' tax filing information.

130. Class members have been damaged by Meta's invasion of their privacy and are entitled to just compensation and injunctive relief.

COUNT VI
Intrusion Upon Seclusion

131. Plaintiffs incorporate the paragraphs contained above as if fully set forth herein.

132. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclass against Defendant.

133. In carrying out this scheme to track and intercept tax filing information, Meta intentionally intruded upon class members' solicitude or seclusion in that it effectively placed itself in the middle of conversation to which it was not an authorized party.

134. Meta's tracking and interception were not authorized by class members.

135. Meta's intentional intrusion into their internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

136. Secret monitoring of tax filing information is highly offensive behavior.

137. Wiretapping and surreptitiously recording of communications is highly offensive behavior.

138. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is preparing their tax filings.

139. Class members have been damaged by Meta's intrusion upon their seclusion and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Meta, as follows:

a. For an order certifying the putative class and subclass and naming Plaintiffs as the representatives of the putative class and subclass and Plaintiffs' attorneys as Class Counsel to represent the putative class and subclass members;

b. For an order declaring that the Defendant's conduct violates the statutes referenced herein;

c. For an order finding in favor of Plaintiffs and the putative class and subclass on all counts asserted herein;

d. For statutory damages in amounts to be determined by the Court and/or jury;

e. For prejudgment interest on all amounts awarded;

f. For injunctive relief as pleaded or as the Court may deem proper; and

g. For an order awarding Plaintiffs and the putative class and subclass their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: December 29, 2022

BURSOR & FISHER, P.A.

By: */s/ Joel D. Smith*

Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: jsmith@bursor.com

Attorneys for Plaintiffs